PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-227298
(43)Date of publication of application : 24.08.1999

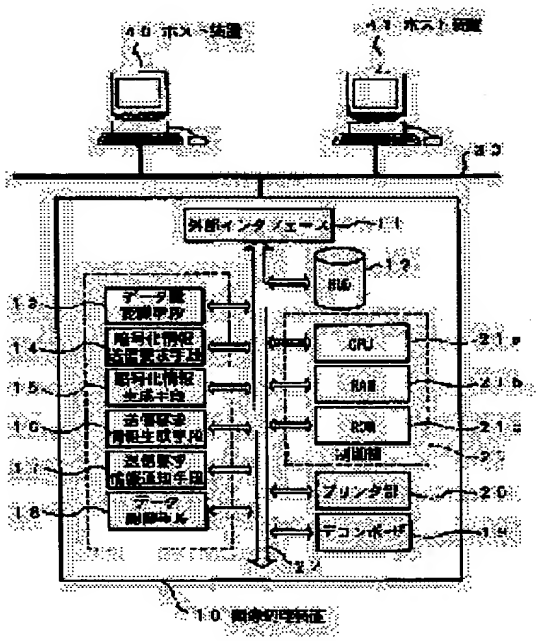
(51)Int.Cl. B41J 29/38
G06F 3/12
G06F 13/00
H04L 9/32

(21)Application number : 10-032927
(22)Date of filing : 16.02.1998

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : EGUCHI HIROYUKI

(54) IMAGE PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To output a data quickly without causing any lowering of throughput due to encryption of data even when a high volume data or a high priority data is outputted.
SOLUTION: This image processor 10 for decrypting a encrypted data from host units 40, 41,... and outputting a visible image comprises means 13 for receiving a data to be outputted after making a decision whether the data satisfies specified conditions or not, and means 14 for requesting the host units 40, 41,... transmitting the data to encrypt the data only when the specified conditions are satisfied.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－227298

(43)公開日　平成11年(1999) 8月24日

(51)Int.Cl.[6]	識別記号	FI	
B41J 29/38		B41J 29/38	Z
G06F 3/12		G06F 3/12	A
			C
13/00	351	13/00	351Z
H04L 9/32		H04L 9/00	675A

審査請求　未請求　請求項の数4　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－32927

(22)出願日　平成10年(1998) 2月16日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　江口　博行
神奈川県海老名市本郷2274番地　富士ゼロックス株式会社海老名事業所内

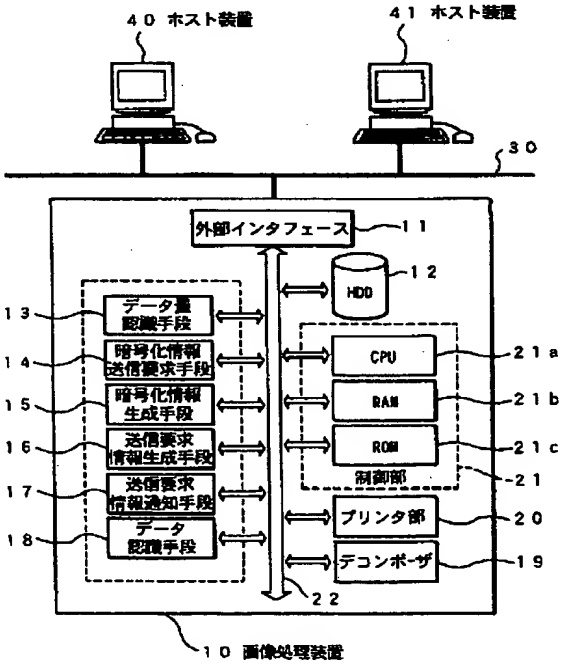
(74)代理人　弁理士　船橋　國則

(54)【発明の名称】　画像処理装置

(57)【要約】

【課題】　データ量の多いデータや出力優先度の高いデータを出力する場合であっても、データの暗号化によるスループットの低下を招くことがなく、迅速なデータ出力を可能とする。

【解決手段】　上位装置４０，４１…からのデータが暗号化されている場合にはこれを解読した後に可視画像として出力する画像処理装置１０において、出力すべきデータを受け取るのに先立ちそのデータが所定条件に該当するか否かを判断する判断手段１３と、所定条件に該当する場合にのみ前記出力すべきデータの送信元の上位装置４０，４１…にそのデータに対する暗号化を要求する要求手段１４とを備える。



1

【特許請求の範囲】
【請求項１】　上位装置に接続され、該上位装置から送信されるデータを受け取ると該データを可視画像として出力するとともに、前記上位装置からのデータが暗号化されている場合にはこれを解読した後に出力を行う画像処理装置において、
出力すべきデータを受け取るのに先立ち、該データが所定条件に該当するか否かを判断する判断手段と、
前記判断手段が所定条件に該当すると判断した場合にのみ、前記出力すべきデータの送信元の上位装置に該データに対する暗号化を要求する要求手段とを備えることを特徴とする画像処理装置。
【請求項２】　前記判断手段は、前記出力すべきデータのデータ量を認識し、その認識結果が所定量以下である場合に該データが所定条件に該当すると判断するものであることを特徴とする請求項１記載の画像処理装置。
【請求項３】　前記判断手段は、前記出力すべきデータの出力優先度を認識し、その認識結果が所定値より低い場合に該データが所定条件に該当すると判断するものであることを特徴とする請求項１記載の画像処理装置。
【請求項４】　前記出力すべきデータの送信元の上位装置に該データに対する暗号化を要求するか否かを選択するための選択設定手段が設けられたことを特徴とする請求項１，２または３記載の画像処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えばネットワークプリンタのように、ネットワーク上において用いられ、受信したデータを可視画像として出力する画像処理装置に係わり、特にセキュリティ確保のために暗号化されたデータについても対応可能である画像処理装置に関するものである。
【０００２】
【従来の技術】近年、インターネットと呼ばれる広域ネットワークシステム等の急激な広がりにより、ネットワーク内におけるデータ通信が頻繁に行われるようになっている。これに伴い、ネットワーク内で通信されるデータへの不正アクセスの防止や、データの発信元と送信先との間の認証等のために、データのセキュリティに関する様々な技術が提案されている。
【０００３】例えば特開平６－４４１２２号公報には、ネットワーク内で通信されるデータを暗号化することにより、不正アクセスや不正利用の防止を徹底したものが開示されている。これによると、ネットワーク内で画像出力を行う画像処理装置は、ホストコンピュータやプリンタサーバ等の上位装置から送信されるデータを出力するのに際し、上位装置との間で暗号化情報の授受を行うようになっている。詳しくは、画像処理装置では、データの送信元となる上位装置に対してそのデータのセキュリティ機能の使用許可を問い合わせた後に、上位装置から暗号化キーが付加されたデータを暗号化情報として受信する。そして、受信した暗号化情報を解読するための演算を行って出力すべきデータを得た後に、その出力すべきデータを可視画像として出力する。

2

【０００４】
【発明が解決しようとする課題】しかしながら、上述した従来の画像処理装置では、上位装置が所定単位のデータ毎、例えば画像処理装置へ送信するメディア（文字、図形、音声、静止画、動画像など）毎に、暗号化キーを付加してこれを暗号化情報とするため、データを出力するのにあたって、暗号化情報を解読するための演算を頻繁に行うこととなる。したがって、例えば、データ量の多いデータ（ページ数の多い文書等）を出力する場合には、暗号化情報を解読するための演算に多くの時間を必要とし、結果として迅速なデータ出力を行うことができなくなってしまう。また、例えば、ネットワーク内でデータの出力優先度を設定可能となっている場合に、出力優先度の高いデータ（緊急を要する文書等）であっても、暗号化情報を解読するための演算によって、これを出力するまでに多くの時間を費やしてしまう可能性がある。
【０００５】つまり、上述した従来の画像処理装置では、出力すべきデータのすべてに暗号化が行われるので、例えばデータ量の多いデータや出力優先度の高いデータを出力する場合に、暗号化解読のために多くの時間を要してしまい、結果として装置としてのスループットが低下してしまうこととなる。
【０００６】そこで、本発明は、例えばデータ量の多いデータや出力優先度の高いデータを出力する場合であっても、データの暗号化によるスループットの低下を招いてしまうことがなく、迅速なデータ出力を行うことのできる画像処理装置を提供することを目的とする。
【０００７】
【課題を解決するための手段】本発明は、上記目的を達成するために案出された画像処理装置で、上位装置に接続され、その上位装置から送信されるデータを受け取るとこのデータを可視画像として出力するとともに、前記上位装置からのデータが暗号化されている場合にはこれを解読した後に出力を行う画像処理装置において、出力すべきデータを受け取るのに先立ち、そのデータが所定条件に該当するか否かを判断する判断手段と、前記判断手段が所定条件に該当すると判断した場合にのみ、前記出力すべきデータの送信元の上位装置にそのデータに対する暗号化を要求する要求手段とを備えることを特徴とするものである。
【０００８】上記構成の画像処理装置によれば、出力すべきデータを受け取るのに先立ち、判断手段が、そのデータが所定条件に該当するか否かを判断する。ここで、例えばそのデータのデータ量が所定量以下であったり出力優先度が所定値より低い場合のように、そのデータが

所定条件に該当すると判断手段が判断すれば、要求手段は、出力すべきデータの送信元の上位装置にそのデータに対する暗号化を要求する。つまり、出力すべきデータが所定条件に該当していなければ、そのデータに対する暗号化を要求しない。したがって、この画像処理装置では、例えばデータ量が所定量より多いデータや出力優先度が所定値より高いデータのように、所定条件に該当しないデータを出力する場合に、そのデータに対する暗号化を解読する必要がなくなる。

【０００９】

【発明の実施の形態】以下、図面に基づき本発明に係わる画像処理装置について説明する。

【００１０】〔第１の実施の形態〕図１は、本発明に係わる画像処理装置の第１の実施の形態の概略構成を示すブロック図である。図例のように、本実施の形態の画像処理装置１０は、ＬＡＮ（ローカルエリアネットワーク）等のネットワーク３０を介して、複数のホスト装置４０，４１…と接続されているものである。

【００１１】ホスト装置４０，４１…は、それぞれがパーソナルコンピュータやワークステーション等からなるものであり、画像処理装置１０で出力すべき印刷データと、この印刷データの属性に関する情報（例えばデータ名、データサイズ、ホスト装置名、ユーザ名等、以下この情報を属性情報と称す）とを、画像処理装置１０に対して送信するものである。これら印刷データおよび属性情報は、各ホスト装置４０，４１…にインストールされているアプリケーションソフトウエア等により作成され、画像処理装置１０へ送信される。なお、印刷データとしては、例えばアスキー（ASCII)コード等によって記述されたものがある。

【００１２】また、各ホスト装置４０，４１…は、詳細を後述するように、それぞれが印刷データの暗号化に必要な暗号化キー情報（以下、暗号化キー＃１と称す）と、暗号化情報の生成および解読に必要なアルゴリズムを予め備えているものとする。なお、暗号化キー＃１は、各ホスト装置４０，４１…毎に個別のものとなっている。

【００１３】このようなホスト装置４０，４１…に接続される画像処理装置１０は、ネットワークプリンタ等からなるものであり、ホスト装置４０，４１…から送信される印刷データを受け取ると、その印刷データを可視画像として記録用紙上に出力するものである。そのために、画像処理装置１０は、外部インタフェース１１と、ハードディスク装置（Hard Disk Drive;以下、ＨＤＤと称す）１２と、データ量認識手段１３と、暗号化情報送信要求手段１４と、暗号化情報生成手段１５と、送信要求情報生成手段１６と、送信要求情報通知手段１７と、データ認識手段１８と、デコンポーザ１９と、プリンタ部２０と、制御部２１と、これらを互いに接続する内部バス２２と、を備えている。

【００１４】ここで、これらの各部について詳しく説明する。外部インタフェース１１は、ネットワークと接続し、このネットワーク３０を介してホスト装置４０，４１…との間の通信を行うためのものである。ＨＤＤ１２は、外部インタフェース１１がホスト装置４０，４１…からの印刷データを受信すると、その印刷データを記憶蓄積するものである。

【００１５】データ量認識手段１３は、ホスト装置４０，４１…から送られてくる印刷データのデータ量を、その印刷データに先立って送られてきた属性情報から抽出し、抽出したデータ量と予め制御部２１内のメモリ等に設定されている所定量と比較して、印刷データのデータ量が所定量以下であるか否かを判断するものである。なお、所定量は、この画像処理装置１０を使用するユーザが任意に変更できるようにしてもよい。

【００１６】暗号化情報送信要求手段１４は、データ量認識手段１３による判断結果に応じて、印刷データの暗号化を許可するか否かのメッセージを、印刷データの送信元のホスト装置４０，４１…に通知するものである。例えば、暗号化情報送信要求手段１４では、データ量認識手段１３が印刷データのデータ量が所定量以下と判断すると、送信元のホスト装置４０，４１…に印刷データの暗号化を許可し、その印刷データに対する暗号化情報の付加を要求する。また、暗号化情報送信要求手段１４では、暗号化の要求の応答として、送信元のホスト装置４０，４１…から暗号化情報を生成するための暗号化キー＃１を取得するようになっている。

【００１７】暗号化情報生成手段１５は、暗号化情報送信要求手段１４が取得した暗号化キー＃１と、予め制御部２１内のメモリ等に保持されている暗号化キー情報（以下、暗号化キー＃２と称す）とを基に、所定の暗号化情報生成アルゴリズムに従って演算を行い、その演算によって暗号化情報を生成するものである。なお、暗号化情報およびこれを生成するための暗号化情報生成アルゴリズムは、周知技術を利用したものであるため、ここではその詳細な説明を省略する。

【００１８】送信要求情報生成手段１６は、ＨＤＤ１２あるいは図示しないバッファメモリの空き容量を基にホスト装置４０，４１…から受信可能な印刷データのデータサイズを算出し、そのデータサイズに関する情報と暗号化情報とから送信要求情報を生成するものである。送信要求情報通知手段１７は、送信要求情報生成手段１６が生成した送信要求情報をホスト装置４０，４１…に送信するものである。

【００１９】データ認識手段１８は、ホスト装置４０，４１…から暗号化された印刷データが送られてくると、その印刷データから暗号化情報を抽出し、抽出した暗号化情報に対して所定の暗号化情報照合アルゴリズムに従って演算を行い、その演算結果から暗号化情報が正しいか否かを照合し、送られてきた印刷データに対する認証

を行うものである。なお、暗号化情報照合アルゴリズムも、暗号化情報生成アルゴリズムと同様に、周知技術を利用したものであるため、ここではその詳細な説明を省略する。

【００２０】デコンポーザ１９は、ホスト装置４０，４１…から受け取った印刷データに対して、可視画像として出力するために必要な処理を行うものである。例えば、デコンポーザ１９では、ＨＤＤ１２から順次取り出したアスキーコード等の印刷データを、プリンタ部２０で出力可能なビットマップデータ等の画像データに変換するようになっている。プリンタ部２０は、デコンポーザ１９が変換した画像データを、周知の電子写真技術を利用して記録用紙上に可視画像として出力するものである。

【００２１】制御手段２１は、上述した各部、すなわち画像処理装置１０全体の動作制御を行うものである。そのために、制御手段２１では、ＣＰＵ（Central ProcessingUnit）２１ａ，ＲＡＭ（Random Access Memory）２１ｂおよびＲＯＭ（Read Only Memory）２１ｃを有している。なお、上述した各手段１３～１８は、この制御手段２１での所定プログラムの実行により、機能的に実現されるものである。

【００２２】次に、以上のように構成された画像処理装置１０において、ホスト装置４０，４１…からの印刷データを出力する場合の処理動作例について、図２および図３のフローチャートを参照しながら説明する。ただし、ここでは、説明を簡単にするために、ネットワーク３０上におけるある１つのホスト装置４０から印刷データの出力依頼があった場合を例に挙げて説明する。

【００２３】ホスト装置４０は、印刷データの出力依頼を行う場合に、先ず、印刷データの送信に先立ち、その印刷データについての属性情報を画像処理装置１０へ送信する。ホスト装置４０が属性情報を送信すると、画像処理装置１０では、図２に示すように、外部インタフェース１１がその属性情報を受信して（ステップ１０１、以下ステップをＳと略す）、その属性情報を制御部２１内のＲＡＭ２１ｂに一時的に格納させる（Ｓ１０２）。

【００２４】属性情報がＲＡＭ２１ｂに格納されると、続いて、画像処理装置１０では、データ量認識手段１３がその属性情報を基に、ホスト装置４０から送られてくる印刷データのデータ量を抽出し（Ｓ１０３）、抽出したデータ量を予め設定されている所定量と比較する（Ｓ１０４）。このとき、抽出したデータ量が所定量よりも小さければ、暗号化情報送信要求手段１４は、印刷データの暗号化を許可する旨のメッセージをホスト装置４０に送信し、その印刷データに対する暗号化情報の付加を要求する（Ｓ１０５）。

【００２５】一方、ホスト装置４０では、印刷データの暗号化を許可する旨のメッセージを受け取ると、そのメッセージに応じて、このホスト装置４０が予め備えている暗号化キー＃１を、画像処理装置１０に対して送信する。

【００２６】ここで、ホスト装置４０からの暗号化キー＃１を外部インタフェース１１が受信すると（Ｓ１０６）、暗号化情報生成手段１５は、その暗号化キー＃１と、予め画像処理装置１０側で保持していた暗号化キー＃２とを基に、暗号化生成アルゴリズムに従って暗号化情報（以下、この暗号化情報を第１の暗号化情報と称す）を生成する（Ｓ１０７）。次いで、送信要求情報生成手段１６は、その時点において受信可能な印刷データのサイズを算出して、これをホスト装置４０に送信を要求する印刷データのサイズとする（Ｓ１０８）。そして、送信要求情報生成手段１６は、その印刷データのサイズに関する情報と先に暗号化情報生成手段１５が生成した第１の暗号化情報とから送信要求情報を生成する（Ｓ１０９）。その後、送信要求情報通知手段１７は、その送信要求情報をホスト装置４０に送信して、その内容をホスト装置４０に通知する（Ｓ１１０）。

【００２７】送信要求情報をホスト装置４０に送信すると、画像処理装置１０では、ホスト装置４０からの印刷データの受信待ち状態となる（Ｓ１１１）。このとき、ホスト装置４０では、送信要求情報を受け取ると、このホスト装置４０が備えるアルゴリズムに従って、送信要求情報に含まれる第１の暗号化情報が正しいか否かの照合、すなわち送信要求情報に対する認証を行う。そして、その照合結果が正しければ、このホスト装置４０の暗号化キー＃１およびアルゴリズムにより、第１の暗号化情報から新たな暗号化情報（以下、この暗号化情報を第２の暗号化情報と称す）を生成するとともに、画像処理装置１０で出力すべき印刷データのうちの送信要求情報で指定されたサイズ分に第２の暗号化情報を付加し、これを画像処理装置１０へ送信する。なお、第２の暗号化情報は、第１の暗号化情報と出力すべき印刷データとから生成するようにしてもよい。

【００２８】その後、ホスト装置４０からの印刷データ（第２の暗号化情報を含む）を外部インタフェース１１が受信すると、制御部２１は、これらをＨＤＤ１２内に記憶蓄積する（Ｓ１１２）。そして、データ認識手段１８は、ＨＤＤ１２内の印刷データから第２の暗号化情報を抽出するとともに（Ｓ１１３）、暗号化情報照合アルゴリズムに従って、その第２の暗号化情報が正しいか否かの照合、すなわち印刷データに対する認証を行う（Ｓ１１４）。

【００２９】このとき、第２の暗号化情報が正しくなければ、制御部２１は、ＨＤＤ１２内の印刷データを破棄する（Ｓ１１５）。また、第２の暗号化情報が正しければ、制御部２１は、ＨＤＤ１２内から印刷データを読み出して（Ｓ１１６）、その印刷データをデコンポーザ１９に転送する（Ｓ１１７）。そして、デコンポーザ１９がその印刷データを画像データに変換するとともに（Ｓ

１１８）、プリンタ部２０がその画像データを記録用紙上に出力する（Ｓ１１９）。制御部２１は、ＨＤＤ１２内の印刷データの全てについて終了するまで、これらのステップ（Ｓ１１６～Ｓ１２０）を繰り返す。

【００３０】これらのステップ（Ｓ１１６～Ｓ１２０）が終了すると、次に、制御部２１は、先にデータ量認識手段１３が認識した印刷データのデータ量の全てについて、ホスト装置４０からの受信が終了しているか否かを判断し（Ｓ１２１）、終了していなければ、再び未受信の印刷データを受信するステップ（Ｓ１１１）から上述したステップを繰り返し、データ量の全てについて終了するまでこれを続行する（Ｓ１１１～Ｓ１２１）。

【００３１】また、データ量認識手段１３による判断の結果（Ｓ１０４）、抽出したデータ量が所定量よりも大きければ、図３に示すように、暗号化情報送信要求手段１４によるメッセージの送信や暗号化情報生成手段１５による第１の暗号化情報の生成を行わずに、送信要求情報生成手段１６が算出した受信可能な印刷データサイズを（Ｓ１２２）、そのままの状態で（第１の暗号化情報を付加せずに）ホスト装置４０へ送信する（Ｓ１２３）。ここで、画像処理装置１０では、ホスト装置４０からの印刷データの受信待ち状態となる（Ｓ１２４）。

【００３２】その後、ホスト装置４０からの印刷データを外部インタフェース１１が受信すると、制御部２１は、これをＨＤＤ１２内に記憶蓄積する（Ｓ１２５）。ただし、このとき、ホスト装置４０からは、指定したサイズの印刷データのみが送信され、第２の暗号化情報については送信されない。これは、暗号化情報送信要求手段１４による暗号化情報の付加要求、具体的には送信要求情報生成手段１６からホスト装置４０への第１の暗号化情報の送信が行われていないからである。

【００３３】そして、制御部２１は、ＨＤＤ１２内から印刷データを読み出して（Ｓ１２６）、デコンポーザ１９による画像データへの変換を経て（Ｓ１２７，Ｓ１２８）、プリンタ部２０での出力を行わせる（Ｓ１２９）。制御部２１は、これをＨＤＤ１２内の印刷データの全てについて終了するまで繰り返し（Ｓ１２４～Ｓ１３０）、さらにはホスト装置４０から受信すべき印刷データの全てについて終了するまで上述したステップを繰り返す（Ｓ１２４～Ｓ１３１）。

【００３４】以上のように、本実施の形態の画像処理装置１０では、出力すべき印刷データのデータ量が所定量以下である場合にのみ、その印刷データの送信元のホスト装置４０，４１…に暗号化を要求するようになっている。すなわち、出力すべき印刷データのデータ量が所定量よりも多ければ、その印刷データに対する暗号化情報の付加を要求しないので、その印刷データの出力に際し、暗号化情報の照合、すなわち暗号化の解読を行う必要がない。

【００３５】したがって、この画像処理装置１０を用いれば、データ量の多い印刷データ（ページ数の多い文書等）を出力する場合には、暗号化解読のための演算を頻繁に行う必要がなくなり、そのために多くの時間を費やしてしまうこともないので、従来よりも迅速な印刷データの出力を行うことができるようになる。これは、特に、ホスト装置４０，４１…との間で所定単位の印刷データ毎、例えば画像処理装置へ送信するメディア（文字、図形、音声、静止画、動画像など）毎に、暗号化を行うように構成されている場合に有効である。

【００３６】つまり、この画像処理装置１０では、出力すべき印刷データのデータ量が所定量よりも多い場合であっても、印刷データの暗号化によるスループットの低下を防ぐことが可能となるので、従来よりも迅速な印刷データの出力を実現することができるようになる。

【００３７】なお、本実施の形態では、画像処理装置１０がホスト装置４０，４１…からの印刷データを出力する場合を例に挙げて説明したが、本発明はこれに限定されるものではない。例えば、図４に示すように、ＬＡＮ３０上にサーバ装置５０が設けられているシステムについても、本発明は適用可能である。この場合、ホスト装置４０，４１…からの印刷データは、サーバ装置５０により識別番号が割り当てられた後に、サーバ装置５０内のプリントキューに蓄えられ、画像処理装置１０での出力が可能であるとサーバ装置５０が判断すると、プリントキュー内から順次画像処理装置１０へ送信される。よって、このようなシステムにおいても、画像処理装置１０がサーバ装置５０からの印刷データのデータ量に応じて、そのデータ量が所定量以下である場合にのみ、サーバ装置５０における暗号化キー＃１（パブリックキー）と画像処理装置１０における暗号化キー＃２（プライベートキー）とに基づく暗号化を行うようにすれば、上述した場合と同様の効果を得ることができる。

【００３８】また、本実施の形態では、印刷データのデータ量に応じて暗号化を要求するか否かを判断する場合を例に挙げて説明したが、本発明はこれに限定されるものではない。例えば、ホスト装置４０，４１…において印刷データの出力の緊急度を表す出力優先度が設定されるとともに、その出力優先度に応じて画像処理装置１０（またはサーバ装置５０）が印刷データの処理順序を決定するように構成された場合に、画像処理装置１０は、属性情報から出力優先度に関する情報を抽出して、これが所定値より低いか否かを判断し、所定値より低ければ暗号化を要求するようにすることも考えられる。このようにすれば、出力優先度の高い印刷データ、すなわち緊急を要する印刷データについては、暗号化解読の演算のために多くの時間を費やしてしまうことがなくなるので、迅速な出力が可能となる。つまり、ユーザの所望する出力（緊急出力等）を実現できるので、ユーザにとっては便利なものとなる。

【００３９】〔第２の実施の形態〕次に、本発明に係わ

る画像処理装置の第２の実施の形態について説明する。ただし、ここでは、上述した第１の実施の形態と同一の構成要素については、同一の符号を与えてその説明を省略し、第１の実施の形態の場合との相違点についてのみ説明する。

【００４０】図５は、本発明に係わる画像処理装置の第２の実施の形態の概略構成を示すブロック図である。図例のように、本実施の形態の画像処理装置１０ａは、第１の実施の形態で説明したものに加えて、液晶タッチパネル２３と、暗号化情報付加手段２４と、が設けられているものである。

【００４１】液晶タッチパネル２３は、画像処理装置１０ａを使用するユーザが操作するためのもので、この画像処理装置１０ａにおけるコンフィグレーション情報の設定やその変更を行うためのものである。この操作手段２３で行う設定の一例としては、ホスト装置４０，４１…からの印刷データについて暗号化を要求するか否かを選択するための設定がある。

【００４２】暗号化情報付加手段２４は、制御手段２１での所定プログラムの実行により、機能的に実現されるものであり、液晶タッチパネル２３での設定結果に応じて、印刷データに対する暗号化を要求するか否かを選択するものである。ただし、暗号化情報付加手段２４では、不揮発性のメモリであるＮＶＲＡＭ（nonvolatileRandom Access Memory）を有しており、このＮＶＲＡＭ内に暗号化を要求するか否かを判断するための暗号化フラグを保持するようになっている。つまり、暗号化情報付加手段２４では、液晶タッチパネル２３での設定結果に応じて変更される暗号化フラグに基づいて、ホスト装置４０，４１…が印刷データを送信する際のセキュリティ機能として暗号化情報を付加するか否かを選択するようになっている。

【００４３】ここで、液晶タッチパネル２３での暗号化を要求するか否かの設定について、図６および図７を参照しながら説明する。図５は、暗号化を要求するか否かを設定する際の液晶タッチパネル２３における表示内容の具体例を示す説明図であり、図６は、暗号化を要求するか否かを設定する際の手順を示すフローチャートである。

【００４４】この画像処理装置１０ａでは、図６（ａ）に示すように、ユーザにより液晶タッチパネル２３上の「メニュー」（アイコン）が押下されると（図７におけるＳ２０１）、液晶タッチパネル２３がメニュー一覧を表示する（図７におけるＳ２０２）。このとき、ユーザにより「メンテナンス」が選択されると（図７におけるＳ２０３）、液晶タッチパネル２３は、図６（ｂ）に示すように、メンテナンスする項目を表示する（図７におけるＳ２０４）。次いで、ユーザによりメンテナンスする項目のうちの「オプションセッテイ」が選択されると（図７におけるＳ２０５）、液晶タッチパネル２３は、図６（ｃ）に示すように、オプション一覧を表示する（図７におけるＳ２０６）。その後、ユーザによりオプション一覧のうちの「アンゴウカ」が選択されると（図７におけるＳ２０７）、液晶タッチパネル２３は、図６（ｄ）に示すように、ユーザに「オン」か「オフ」を選択させる。ここで「オン」が選択され（図７におけるＳ２０８）、その後「スタート」（アイコン）が押下されると（図７におけるＳ２０９）、液晶タッチパネル２３は、「オン」が選択された旨を暗号化情報付加手段２４に通知する。そして、暗号化情報付加手段２４は、液晶タッチパネル２３からの通知に従って、ＮＶＲＡＭ内の暗号化フラグを、「オン」が選択された旨に対応する「１」（TRUE）に書き換える。このようにして、暗号化を要求するか否かの設定が行われる。

【００４５】次に、以上のような画像処理装置１０ａにおいて、ホスト装置４０，４１…からの印刷データを出力する場合の処理動作例について、図８および図９のフローチャートを参照しながら説明する。ただし、ここでも、ある１つのホスト装置４０から印刷データの出力依頼があった場合を例に挙げて説明する。

【００４６】この画像処理装置１０ａでは、上述したように、液晶タッチパネル２３で暗号化を要求するか否かの設定が行われると、図８に示すように、暗号化情報付加手段２４がＮＶＲＡＭ内の暗号化フラグを書き換えて変更することにより、その設定内容を保持しておく（Ｓ３０１）。なお、この暗号化フラグは、次の印刷データを処理するときから反映され、画像処理装置１０ａの電源がオフされても保持される。

【００４７】ここで、ホスト装置４０から属性情報の送信があると、この画像処理装置１０ａでは、第１の実施の形態の場合と同様に、外部インタフェース１１がその属性情報を受信し、ＲＡＭ２１ｂに一時的に格納させる（Ｓ３０２～Ｓ３０３）。

【００４８】ただし、この画像処理装置１０ａでは、ホスト装置４０からの属性情報がＲＡＭ２１ｂに格納されると、第１の実施の形態の場合とは異なり、暗号化情報付加手段２４が暗号化フラグのチェックを行う。詳しくは、暗号化情報付加手段２４は、ＮＶＲＡＭ内の暗号化フラグが「１」（TRUE）であるか否かを判断する（Ｓ３０４）。

【００４９】そして、暗号化フラグが「１」（TRUE）であれば、この画像処理装置１０ａでは、暗号化情報送信要求手段１４が印刷データの暗号化を許可する旨のメッセージをホスト装置４０に送信し（Ｓ３０５）、以下、第１の実施の形態の場合（図２におけるＳ１０６～Ｓ１２１参照）と同様の処理を行う（Ｓ３０６～Ｓ３２１）。また、暗号化フラグが「１」（TRUE）でなければ、この画像処理装置１０ａでは、図９に示すように、暗号化情報送信要求手段１４によるメッセージの送信を行わずに、以下、第１の実施の形態の場合（図３におけ

るＳ１２２～Ｓ１３１参照）と同様の処理を行う（Ｓ３２２～Ｓ３３１）。

【００５０】以上のように、本実施の形態の画像処理装置１０ａでは、液晶タッチパネル２３での暗号化を要求するか否かの設定に応じて、暗号化情報付加手段２４が暗号化フラグを変更するとともに、この暗号化フラグに基づいて暗号化情報送信要求手段１４が印刷データの暗号化を要求するようになっている。すなわち、暗号化を要求するか否かを、液晶タッチパネル２３から選択し得るようになっている。したがって、この画像処理装置１０ａを用いれば、ユーザは、スループットの低下を防いで迅速な出力を実現するか、あるいは印刷データのセキュリティを確保するか、を任意に選択できる。これにより、この画像処理装置１０ａは、ユーザにとっては非常に便利なものになるとともに、システムとしての汎用性を高めることも可能となる。

【００５１】なお、本実施の形態では、液晶タッチパネル２３での設定結果のみに応じて、印刷データに対する暗号化を要求するか否かを選択する場合を例に挙げて説明したが、本発明はこれに限定されるものではなく、第１の実施の形態で説明した場合との組み合わせを実現してもよい。この場合には、例えば、暗号化情報送信要求手段１４が、印刷データのデータ量が所定量以下であり、かつ、暗号化フラグが「１」（TRUE）である場合に、印刷データの暗号化を許可する旨のメッセージをホスト装置４０，４１…に送信することが考えられる。

【００５２】

【発明の効果】以上に説明したように、本発明の画像処理装置は、出力すべき印刷データが所定条件に該当する場合にのみ、その印刷データの送信元の上位装置に暗号化を要求するようになっている。すなわち、印刷データが所定条件に該当しなければ、その印刷データに対する暗号化を要求しない。したがって、所定条件に該当しない印刷データについては、その出力に際し暗号化の解読を行う必要がないので、そのために多くの時間を費やしてしまうことがなく、従来よりも迅速な出力を実現し、スループットが低下してしまうことを防ぐことができる。

【図面の簡単な説明】

【図１】　本発明に係わる画像処理装置の第１の実施の形態の概略構成を示すブロック図である。

【図２】　第１の実施の形態の画像処理装置において印刷データを出力する場合の処理動作例を示すフローチャート（その１）である。

【図３】　第１の実施の形態の画像処理装置において印刷データを出力する場合の処理動作例を示すフローチャート（その２）である。

【図４】　第１の実施の形態の画像処理装置の応用例を示すブロック図である。

【図５】　本発明に係わる画像処理装置の第２の実施の形態の概略構成を示すブロック図である。

【図６】　暗号化を要求するか否かを設定する際の液晶タッチパネルにおける表示内容の具体例を示す説明図であり、（ａ）はメニュー一覧の具体例の図、（ｂ）はメンテナンスする項目の具体例の図、（ｃ）はオプション一覧の具体例の図、（ｄ）は暗号化を要求するか否かの設定画面の具体例の図である。

【図７】　暗号化を要求するか否かを設定する際の手順を示すフローチャートである。

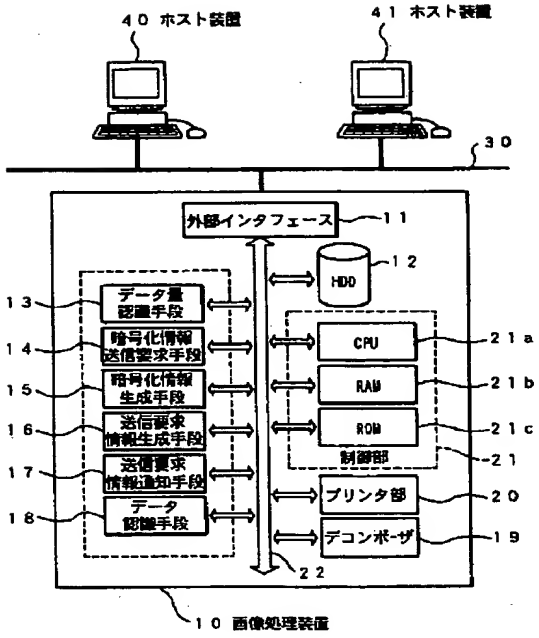
【図８】　第２の実施の形態の画像処理装置において印刷データを出力する場合の処理動作例を示すフローチャート（その１）である。

【図９】　第２の実施の形態の画像処理装置において印刷データを出力する場合の処理動作例を示すフローチャート（その２）である。

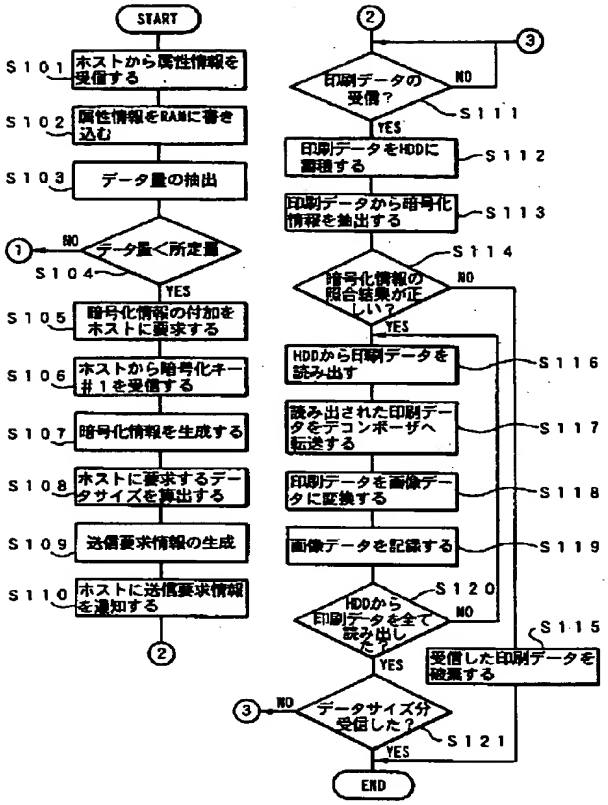
【符号の説明】

１０…画像処理装置、１３…データ量認識手段、１４…暗号化情報送信要求手段、１５…暗号化情報生成手段、１６…送信要求情報生成手段、１７…送信要求情報通知手段、１８…データ認識手段、２３…液晶タッチパネル、２４…暗号化情報付加手段、４０，４１…ホスト装置、５０…サーバ装置

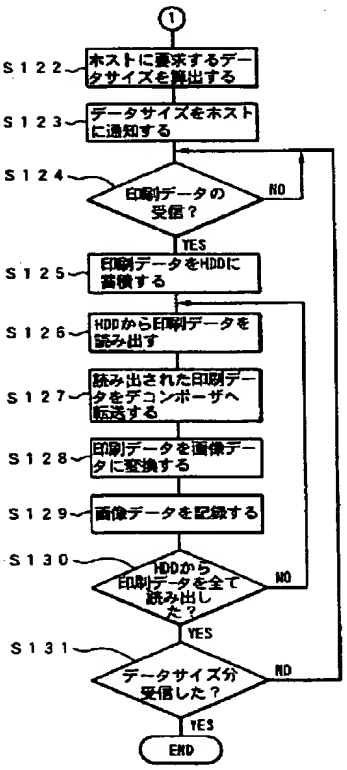
【図１】


４０ ホスト装置
４１ ホスト装置
３０
外部インタフェース
１１
１２
HDD
１３
データ量認識手段
１４
暗号化情報送信要求手段
１５
暗号化情報生成手段
１６
送信要求情報生成手段
１７
送信要求情報通知手段
１８
データ認識手段
CPU
２１ａ
RAM
２１ｂ
ROM
２１ｃ
制御部
２１
プリンタ部
２０
デコンポーザ
１９
２２
１０ 画像処理装置

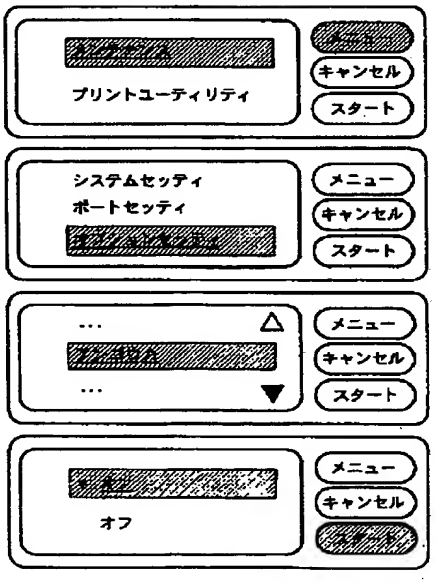
【図２】


START
S101 ホストから属性情報を受信する
S102 属性情報をRAMに書き込む
S103 データ量の抽出
データ量＜所定量
NO
S104
YES
S105 暗号化情報の付加をホストに要求する
S106 ホストから暗号化キー#1を受信する
S107 暗号化情報を生成する
S108 ホストに要求するデータサイズを算出する
S109 送信要求情報の生成
S110 ホストに送信要求情報を通知する
印刷データの受信？
NO
S111
YES
印刷データをHDDに蓄積する
S112
印刷データから暗号化情報を抽出する
S113
暗号化情報の照合結果が正しい？
S114
NO
YES
HDDから印刷データを読み出す
S116
読み出された印刷データをデコンポーザへ転送する
S117
印刷データを画像データに変換する
S118
画像データを記録する
S119
HDDから印刷データを全て読み出した？
S120
NO
YES
S115
受信した印刷データを破棄する
データサイズ分受信した？
NO
S121
YES
END

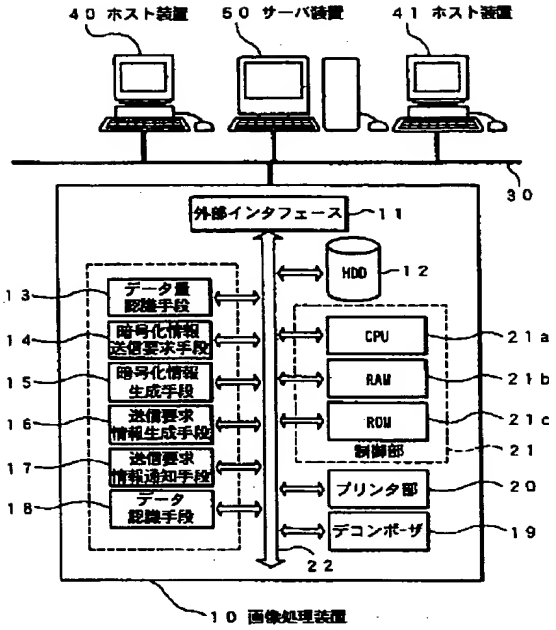
【図３】


S122 ホストに要求するデータサイズを算出する
S123 データサイズをホストに通知する
S124 印刷データの受信？
NO
YES
S125 印刷データをHDDに蓄積する
S126 HDDから印刷データを読み出す
S127 読み出された印刷データをデコンポーザへ転送する
S128 印刷データを画像データに変換する
S129 画像データを記録する
S130 HDDから印刷データを全て読み出した？
NO
YES
S131 データサイズ分受信した？
NO
YES
END

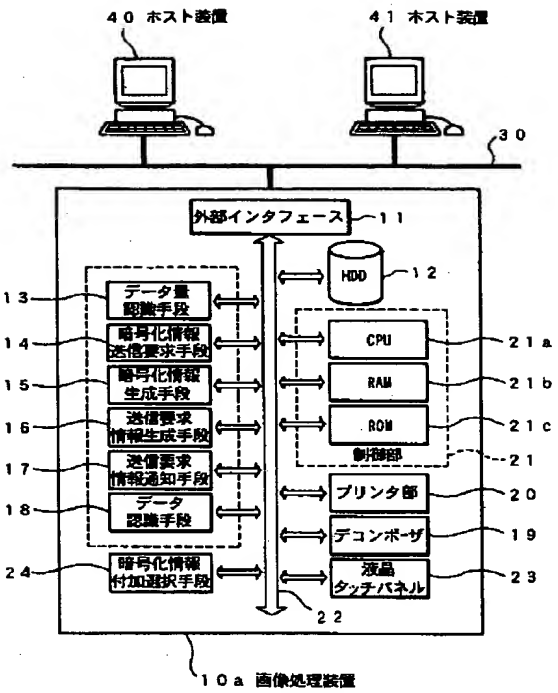
【図６】


(a)
プリントユーティリティ
メニュー
キャンセル
スタート
(b)
システムセッティ
ポートセッティ
メニュー
キャンセル
スタート
(c)
メニュー
キャンセル
スタート
(d)
オフ
メニュー
キャンセル

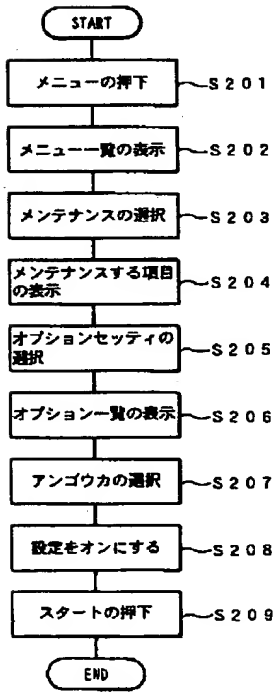
【図４】


４０ ホスト装置
５０ サーバ装置
４１ ホスト装置
３０
外部インタフェース
１１
HDD
１２
１３
データ量認識手段
１４
暗号化情報送信要求手段
１５
暗号化情報生成手段
１６
送信要求情報生成手段
１７
送信要求情報通知手段
１８
データ認識手段
CPU
２１ａ
RAM
２１ｂ
ROM
２１ｃ
制御部
２１
プリンタ部
２０
デコンポーザ
１９
２２
１０ 画像処理装置

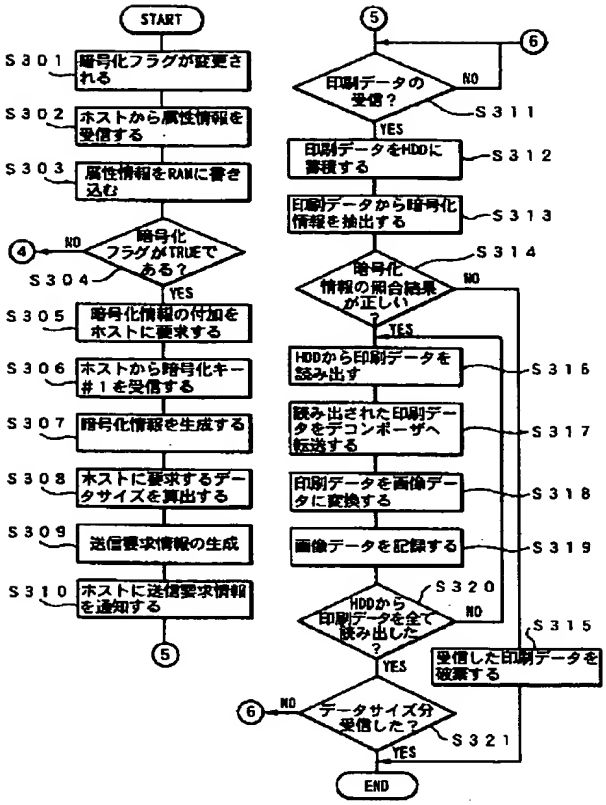
【図５】


４０ ホスト装置
４１ ホスト装置
３０
外部インタフェース
１１
HDD
１２
１３
データ量認識手段
１４
暗号化情報送信要求手段
１５
暗号化情報生成手段
１６
送信要求情報生成手段
１７
送信要求情報通知手段
１８
データ認識手段
２４
暗号化情報付加選択手段
CPU
２１ａ
RAM
２１ｂ
ROM
２１ｃ
制御部
２１
プリンタ部
２０
デコンポーザ
１９
液晶タッチパネル
２３
２２
１０ａ 画像処理装置

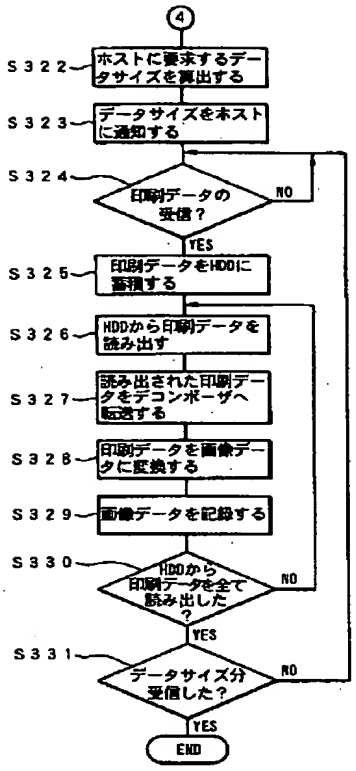
【図７】


START
メニューの押下
Ｓ２０１
メニュー一覧の表示
Ｓ２０２
メンテナンスの選択
Ｓ２０３
メンテナンスする項目の表示
Ｓ２０４
オプションセッティの選択
Ｓ２０５
オプション一覧の表示
Ｓ２０６
アンゴウカの選択
Ｓ２０７
設定をオンにする
Ｓ２０８
スタートの押下
Ｓ２０９
END

【図８】


START
S301 暗号化フラグが変更される
S302 ホストから属性情報を受信する
S303 属性情報をRAMに書き込む
S304 暗号化フラグがTRUEである？
NO
YES
S305 暗号化情報の付加をホストに要求する
S306 ホストから暗号化キー#1を受信する
S307 暗号化情報を生成する
S308 ホストに要求するデータサイズを算出する
S309 送信要求情報の生成
S310 ホストに送信要求情報を通知する
S311 印刷データの受信？
S312 印刷データをHDDに蓄積する
S313 印刷データから暗号化情報を抽出する
S314 暗号化情報の照合結果が正しい？
S315 受信した印刷データを破棄する
S316 HDDから印刷データを読み出す
S317 読み出された印刷データをデコンポーザへ転送する
S318 印刷データを画像データに変換する
S319 画像データを記録する
S320 HDDから印刷データを全て読み出した？
S321 データサイズ分受信した？
END

【図９】


S322 ホストに要求するデータサイズを算出する
S323 データサイズをホストに通知する
S324 印刷データの受信？
S325 印刷データをHDDに蓄積する
S326 HDDから印刷データを読み出す
S327 読み出された印刷データをデコンポーザへ転送する
S328 印刷データを画像データに変換する
S329 画像データを記録する
S330 HDDから印刷データを全て読み出した？
S331 データサイズ分受信した？
NO
YES
END